AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A countermeasure method against attacks by differential analysis in an electronic component implementing a secret key cryptographic algorithm, the implementation of which comprises a number of successive calculation cycles in order to supply, from first input data applied to the first cycle, final data at the output of the last cycle to produce an encrypted message, each calculation cycle using calculation means for supplying an output data item from an input data item, said calculation means performing the ~~steps~~ step of:

applying ~~a first~~ at least one random value to the input data item and to the output data item in order to obtain an unpredictable data item as an output,

and wherein said countermeasure method includes the further step of:

applying a second random value to said first input data by means of an EXCLUSIVE OR operation.

2. (Previously Presented) A countermeasure method according to Claim 1, further including the step of applying the second random value to the final data supplied by the last cycle by means of an EXCLUSIVE OR operation.

3. (Currently Amended) A countermeasure method according to claim 1 further including the step, at the end of each cycle, of executing an additional operation to eliminate said ~~first~~ one random value at the output of each cycle.

4. (Previously Presented) A countermeasure method according to claim 1 wherein a new set of first and second random values is selected for each new execution of the algorithm.

5. (Currently Amended) A method according to Claim 4, wherein said calculation means are ~~calculated~~ derived from first calculation means ~~defining, for input data~~, which defines corresponding output data for input data, said derivation being obtained by applying the second random value to said input data and applying the first random value at least to said output data of the first calculation means.

6. (Previously Presented) A countermeasure method according to Claim 5, wherein the calculation means comprise constants tables.

7. (Amended) An electronic security component that implements a countermeasure method for attacks against a secret key cryptographic algorithm by means of differential analysis, wherein said algorithm comprises a number of successive calculation cycles in order to supply, from first input data applied to the first cycle, final data at the output of the last cycle to produce an encrypted message, each calculation cycle using calculation means for supplying an output data item from an input data item, said ~~calculation means comprising the application of a first random value to the input data item and to the output data item to obtain an unpredictable output data item,~~ component comprising first calculation means fixed in a program memory, second calculation means that are calculated at each new

execution of the algorithm and stored in working memory by applying a first random value to the input data item and a second random value to the output data item, and means for generating said first and second random values for calculating said second calculation means.

8. (Original) A smart card comprising an electronic security component according to Claim 7.